In the Claims

Please cancel claims 1—82.

83. (New) A method, at least partially implemented by a computer, comprising:

building a data block comprising a first random value and a cryptographic hash of the first random value;

generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

84. (New) The method as recited in Claim 83, wherein the second computing device is a smart card.

85. (New) The method as recited in Claim 83, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

86. (New) The method as recited in Claim 83, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

87. (New) The method as recited in Claim 83, further comprising:

encrypting the data block using the encryption key; and

storing the encrypted data block and the second and third random values.

88. (New) The method as recited in Claim 87, further comprising:

accessing the stored encrypted data block and the second and third random values;

providing a string containing the second random value to the second computing device; and

generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

89. (New) The method as recited in Claim 88, further comprising:

computing a decryption key using the second signature and the third random value;

decrypting the encrypted data block with the decryption key; and

comparing the decryption of the encrypted data block to the data block.

90. (New) The method as recited in Claim 89, wherein computing the decryption key comprises:

hashing the second signature concatenated to the third random value.

91. (New) The method as recited in Claim 89, further comprising:

hashing the first random value contained within the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value contained within the decryption of the encrypted data block.

92. (New) A method, at least partially implemented by a computer, comprising:

accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

accessing second and third random values;

providing a string containing the second random value to a second computing device;

generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

93. (New) The method as recited in Claim 92, wherein the second computing device is a smart card.

94. (New) The method as recited in Claim 92, wherein computing the decryption key comprises:

hashing the signature concatenated to the third random value.

95. (New) The method as recited in Claim 92, further comprising:

decrypting the encrypted data block with the decryption key, wherein the first random value and the hash of the first random value are recovered by the decryption; and

comparing the first random value and the hash of the first random value recovered from the decryption to a data block from which the encrypted data block was generated.

96. (New) The method as recited in Claim 95, further comprising:

hashing the first random value recovered from the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value recovered from the decryption of the encrypted data block.

97. (New) One or more computer-readable media comprising computer-executable instructions for encryption-based authentication, the computer-executable instructions comprising instructions for:

building a data block comprising a first random value and a cryptographic hash of the first random value;

generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

98. (New) The one or more computer-readable media as recited in Claim 97, wherein the second computing device is a smart card.

99. (New) The one or more computer-readable media as recited in Claim 97, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

100. (New) The one or more computer-readable media as recited in Claim 97, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

101. (New) The one or more computer-readable media as recited in Claim 97, further comprising instructions for:

encrypting the data block using the encryption key; and

storing the encrypted data block and the second and third random values.

102. (New) The one or more computer-readable media as recited in Claim 101, further comprising instructions for:

accessing the stored encrypted data block and the second and third random values;

providing a string containing the second random value to the second computing device; and

generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

103. (New) The one or more computer-readable media as recited in Claim 102, further comprising instructions for:

computing a decryption key using the second signature and the third random value;

decrypting the encrypted data block with the decryption key; and

comparing the decryption of the encrypted data block to the data block.

104. (New) The one or more computer-readable media as recited in Claim 103, wherein computing the decryption key comprises instructions for:

hashing the second signature concatenated to the third random value.

105. (New) The one or more computer-readable media as recited in Claim 103, further comprising instructions for:

hashing the first random value contained within the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value contained within the decryption of the encrypted data block.

106. (New) One or more computer-readable media comprising computer-executable instructions for encryption-based authentication, the computer-executable instructions comprising instructions for:

accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

accessing second and third random values;

providing a string containing the second random value to a second computing device;

generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

107. (New) The one or more computer-readable media as recited in Claim 106, wherein the second computing device is a smart card.

108. (New) The one or more computer-readable media as recited in Claim 106, wherein computing the decryption key comprises instructions for:

hashing the signature concatenated to the third random value.

109. (New) The one or more computer-readable media as recited in Claim 106, further comprising instructions for:

decrypting the encrypted data block with the decryption key, wherein the first random value and the hash of the first random value are recovered by the decryption; and

comparing the first random value and the hash of the first random value recovered from the decryption to a data block from which the encrypted data block was generated.

110. (New) The one or more computer-readable media as recited in Claim 109, further comprising instructions for:

hashing the first random value recovered from the decryption of the encrypted data block; and

comparing the result of this hash with the hash of the first random value recovered from the decryption of the encrypted data block.

111. (New) A system configured for encryption-based authentication, comprising:

means for building a data block comprising a first random value and a cryptographic hash of the first random value;

means for generating, on a second computing device, a signature by digitally signing a string containing a second random value; and

means for computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

112. (New) The system as recited in Claim 111, wherein the second computing device is a smart card.

113. (New) The system as recited in Claim 111, wherein the combination of the digitally signed string and the third random value comprises the digitally signed string concatenated to the third random value.

114. (New) The system as recited in Claim 111, wherein the combination of the digitally signed string and the third random value comprises the third random value concatenated to the digitally signed string.

115. (New) The one or more computer-readable media as recited in Claim 111, further comprising:

means for encrypting the data block using the encryption key; and

means for storing the encrypted data block and the second and third random values.

116. (New) The system as recited in Claim 115, further comprising:

means for accessing the stored encrypted data block and the second and third random values;

means for providing a string containing the second random value to the second computing device; and

means for generating, on the second computing device, a second signature by digitally signing the string containing the second random value.

117. (New) The system as recited in Claim 116, further comprising:

means for computing a decryption key using the second signature and the third random value;

means for decrypting the encrypted data block with the decryption key; and

means for comparing the decryption of the encrypted data block to the data block.

118. (New) The system as recited in Claim 117, wherein computing the decryption key comprises:

means for hashing the second signature concatenated to the third random value.

119. (New) The system as recited in Claim 117, further comprising:

means for hashing the first random value contained within the decryption of the encrypted data block; and

means for comparing the result of this hash with the hash of the first random value contained within the decryption of the encrypted data block.

120. (New) A system configured for encryption-based authentication, comprising:

means for accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value;

means for accessing second and third random values;

means for providing a string containing the second random value to a second computing device;

means for generating, on the second computing device, a signature by digitally signing the string containing the second random value; and

means for computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

121. (New) The system media as recited in Claim 120, wherein the second computing device is a smart card.

122. (New) The system as recited in Claim 120, wherein computing the decryption key comprises:

means for hashing the signature concatenated to the third random value.

123. (New) The system as recited in Claim 120, further comprising:

means for decrypting the encrypted data block with the decryption key, wherein the first random value and the hash of the first random value are recovered by the decryption; and

means for comparing the first random value and the hash of the first random value recovered from the decryption to a data block from which the encrypted data block was generated.

124. (New) The system as recited in Claim 123, further comprising:

means for hashing the first random value recovered from the decryption of the encrypted data block; and

means for comparing the result of this hash with the hash of the first random value recovered from the decryption of the encrypted data block.